This document is scheduled to be published in the
Federal Register on 01/22/2016 and available online at
http://federalregister.gov/a/2016-01169, and on **FDsys.gov**

9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2016-0001]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of an updated and reissued system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0001 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions or privacy issues please contact: Karen L. Neuman, (202-343-1717), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) is giving notice of a proposed rule to accompany an updated system of records notice titled, "DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records."

DHS maintains a synchronized copy of the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI)-019 Terrorist Screening Records System of Records (August 22, 2007, 72 FR 47073) via a technological mechanism called DHS Watchlist Service (WLS) that disseminates the feed to authorized DHS components. The WLS supports an automated and centralized data transmission of TSDB data to DHS. The WLS replaced multiple data feeds from the FBI/TSC to DHS and its components, as

documented by information sharing agreements. The WLS is a system to system secure connection with no direct user interface.

DHS is publishing this notice of proposed rulemaking to account for the expansion of the current system of records notice to clarify one category of individuals and add two new categories of individuals whose information is currently included in, or is contemplated for inclusion in, the TSDB. These categories of information have been included in the TSDB to in support of the White House's "Strategy to Combat Transnational Organized Crime" (July 19, 2011), and National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security" (June 5, 2008). These executive strategies are relevant to DHS's vetting and screening operations.

DHS is clarifying the category of individuals to explicitly include relatives, associates, or others closely connected with a known or suspected terrorist who are excludable from the United States based on these relationships by virtue of sec. 212(a)(3)(B) of the Immigration and Nationality Act, as amended, and do not otherwise satisfy the requirements for inclusion in the TSDB.

DHS is adding two new categories of individuals to include: (1) individuals who were officially detained during military operations, but not as enemy prisoners of war, and who have been identified as possibly posing a threat to national security, and who do not otherwise satisfy the requirements for inclusion in the TSDB ("military detainees"), consistent with E.O. 12333 (or successor order) and the DOJ/FBI-019; and (2) individuals who may pose a threat to national security because they are (a) known or suspected to be or have been engaged in conduct constituting, in aid of, or related to

transnational organized crime, thereby posing a possible threat to national security, and (b) do not otherwise satisfy the requirements for inclusion in the TSDB ("transnational organized crime actors"), consistent with E.O. 12333 (or successor order) ("national security threats") and in support of the White House's "Strategy to Combat Transnational Organized Crime" (July 19, 2011), and National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security" (June 5, 2008).

DHS is also publishing this notice of proposed rulemaking to account for the expansion of the current system of records to clarify and expand the categories of records maintained by the Department. These categories of records are types of data elements included in the TSDB and are shared with DHS and have been deemed relevant to supporting DHS's vetting and screening operations.

1. Identifying biographic information, such as name, date of birth, place of birth, passport or driver's license information, and any other available identifying particulars used to compare the identity of an individual being screened with a subject in the TSDB;
2. Biometric information, such as photographs, fingerprints, or iris images, and associated biographic and contextual information;
3. References to, or information from, other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism and/or national security information, such as unique identification numbers used in other systems;

4. Information collected and compiled to maintain an audit trail of the activity of authorized users of WLS information systems; and
5. System-generated information, including metadata, archived records and record histories from WLS.

DHS is planning future enhancements to the WLS that will provide for a central mechanism to receive information from DHS components when they encounter a potential match to the TSDB and send this information to the FBI/TSC. DHS will update this SORN to reflect such enhancements to the WLS once that capability is implemented. All encounter-related information sharing from DHS to the FBI/TSC will be conducted pursuant to the programmatic system of records notices outlined above.

DHS previously published a Final Rule in the Federal Register to exempt this system of records from certain provisions of the Privacy Act at 75 FR 55335, Dec. 29, 2011. DHS is publishing a new notice of proposed rulemaking to cover the exemptions that will now be applied to these new categories of individuals covered within this system of records. The existing Final Rule for Privacy Act exemptions continues to apply until the new Final Rule is published. This updated system will be included in DHS's inventory of record systems.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records"

is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/ALL-030 Use of the Terrorist Screening Database System of Records. Some information in DHS/ALL-030 Use of the Terrorist Screening Database System of Records relates to official DHS national security and law enforcement activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension. In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case-by-case basis.

A notice of system of records for DHS/ALL-030 Use of the Terrorist Screening Database System of Records is also published elsewhere in this issue of the Federal Register.

List of Subjects in 6 CFR part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 is revised to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. In Appendix C to Part 5, revise paragraph 66 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

66. The DHS/ALL-030 Use of the Terrorist Screening Database System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL-030 Use of the Terrorist Screening Database System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ALL-030 Use of the Terrorist Screening Database

System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or

evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would

alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and

other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

* * * * *

Dated: January 12, 2016.

Karen L. Neuman
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-01169 Filed: 1/21/2016 8:45 am; Publication Date: 1/22/2016]